ABSTRACT

This invention concerns a safe data exchange method between two devices locally connected to one another.

In a preferred embodiment, the first device (10) is a security module containing a first encrypting key, said private key (PAKV) of a pair of asymmetric encrypting keys. The second device is a receiver (11) comprising at least one second encrypting key, said public key (PAKB) of said pair of asymmetric encrypting keys. Furthermore each of the devices comprises a symmetrical key (13). The first device (10) generates a first random number (A), which is encrypted by said private key (PAKV), then transmitted to the second device (11), in which it is decrypted by means of the public key (PAKB). The second device (11) generates a second random number (B), which is encrypted by said public key (PAKB), then transmitted to the first device (10), in which it is decrypted by means of the private key (PAKV). A session key (SK), used for safe data exchange, is generated by a combination of the symmetric key (13) and the random numbers (A, B) generated and received by each of the devices.

(Figure 4)